36/3,K/64 (Item 64 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009006829 **Image available**
WPI Acc No: 1992-134134/199217
XRPX Acc No: N92-100102

Integrated circuit **for** smart card **with improved access control - uses status** monitors **that deliver results to register that is** monitored **at each transaction to** check **for misuse of card**

Patent Assignee: GERONIMI F (GERO-I); GEMPLUS CARD INT SA (GEMP-N)
Inventor: GERONIMI F; SOURENIAN P
Number of Countries: 008 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 481881	A	19920422	EP 91402757	A	19911015	199217	B
FR 2668274	A1	19920424	FR 9012986	A	19901019	199224	
CA 2053741	A	19920420	CA 2053741	A	19911018	199228	
EP 481881	B1	19930324	EP 91402757	A	19911015	199312	
DE 69100052	E	19930429	DE 600052	A	19911015	199318	
			EP 91402757	A	19911015		
ES 2041549	T3	19931116	EP 91402757	A	19911015	199350	
US 5465349	A	19951107	US 91779817	A	19911021	199550	
			US 94384531	A	19941005		
CA 2053741	C	19960716	CA 2053741	A	19911018	199639	

Priority Applications (No Type Date): FR 9012986 A 19901019
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 481881	A	F	6		
Designated States (Regional): DE ES GB IT NL					
CA 2053741	A	F		G06K-019/073	
EP 481881	B1	F	6	G07F-007/10	
Designated States (Regional): DE ES GB IT NL					
DE 69100052	E			G07F-007/10	Based on patent EP 481881
ES 2041549	T3			G07F-007/10	Based on patent EP 481881
US 5465349	A		4	G06F-011/24	Cont of application US 91779817
CA 2053741	C	F		G06K-019/073	
FR 2668274	A1			G06F-012/14	

Integrated circuit **for** smart card **with improved access control...**

...**uses status** monitors **that deliver results to register that is** monitored **at each transaction to** check **for misuse of card**

...Abstract (Basic): The **integrated circuit** has a **microprocessor** with program **memory** (12), non-volatile programmable **memory** (16), an input-output port (18), and a register (RS) storing signals from abnormality **detectors** (C1 to C4). This register is accessible by the **microprocessor** . The register state is verified immediately before each write or erase operation, and before each transmission of data from the input-output port. If verification indicates abnormal conditions, **microprocessor** operation is **interrupted** .

...

...ADVANTAGE - Reduced risk of fraudulent use of **smart cards** .

...Abstract (Equivalent): **Integrated circuit** with **microprocessor** , comprising a program **memory** (12), a programmable non-volatile **memory** (16), at least one input-out-put gate (18) for the **connection** of the

circuit to the outside, safety pick-ups (C1 to C4) to **detect** abnormal operating or environment conditions and a register (RS) accessible by the **microprocessor** and capable of **memorising** an item of information on the state of the pickups, characterised by the fact that...

...the state of the register immediately before each writing or erasing operation of the programmable **memory** and immediately before each transmission of data to the outside via the input-output gate, and means for **interrupting** the operation of the **microprocessor** if a verification of the state of the register brings abnormal conditions to light

...Abstract (Equivalent): An **integrated** **circuit** comprising...

...a first **memory** means for storing application programs...

...a second **memory** means which is programmable and non-volatile, for storing data...

...a plurality of means for continually **sensing** ambient conditions or electrical conditions of the **integrated** **circuit** which fall outside a normal operating range...

...register means for storing **sensing** information from the **sensing** means indicative of said ambient conditions or said electrical conditions of the **integrated** **circuit** which fall outside said normal operating range...

...a **microprocessor** means connected to said first and second **memory** means, said I/O port means, and said register means...

...said first **memory** means storing **test** subroutines for causing said **microprocessor** means to **detect** the presence or absence of said **sensing** information in said register means only in response to requests for the execution of one...

...a) writing data to said second **memory** means...

...b) clearing data from said second **memory** means; or...

...c) transmission of data from said second **memory** means, through the I/O port...

...the **microprocessor** means being **interrupted** if said **sensing** information is found to be present in said register means...

...Title Terms: **MONITOR** ;

US005465349A

United States Patent [19]

Geronimi et al.

[11] **Patent Number: 5,465,349**

[45] **Date of Patent: Nov. 7, 1995**

[54] **SYSTEM FOR MONITORING ABNORMAL INTEGRATED CIRCUIT OPERATING CONDITIONS AND CAUSING SELECTIVE MICROPROCESSOR INTERRUPTS**

[75] Inventors: **Francois Geronimi**, Aix en Provence; **Paul Sourenian**, Marseille, both of France

[73] Assignee: **Gemplus Card International**, Gemenos, France

[21] Appl. No.: **384,531**

[22] Filed: **Oct. 5, 1994**

Related U.S. Application Data

[63] Continuation of Ser. No. 779,817, Oct. 21, 1991, abandoned.

[30] **Foreign Application Priority Data**

Oct. 20, 1990 [FR] France 90 12986

[51] **Int. Cl.^{6}** **G06F 11/24**; G06F 11/30; G06F 12/14

[52] **U.S. Cl.** **364/550**; 395/183.1; 395/184.01; 395/186; 395/183.06

[58] **Field of Search** 365/228; 395/425, 395/575, 725

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,827,149	5/1989	Yabe	307/64
4,939,353	7/1990	Iijima	235/438
5,204,840	4/1993	Mazur	365/228
5,206,938	4/1993	Fujioka	395/400
5,218,607	6/1993	Saito et al.	371/66

FOREIGN PATENT DOCUMENTS

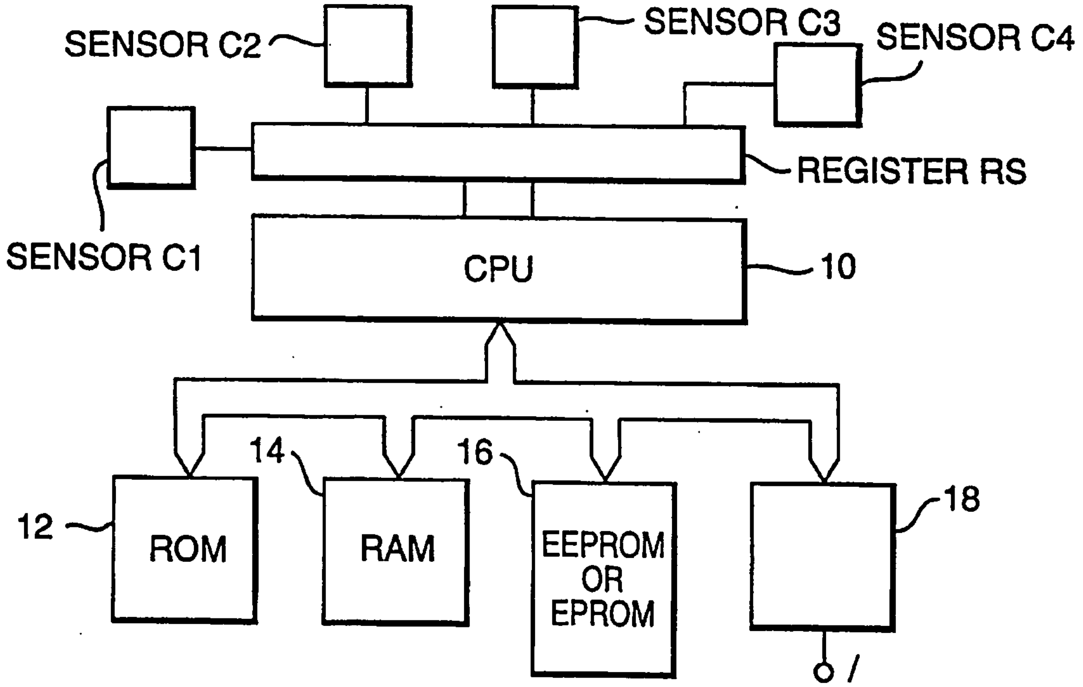
0341712	4/1990	European Pat. Off. .
3706466	6/1987	Germany .

Primary Examiner—David L. Robertson
Assistant Examiner—B. James Peikari
Attorney, Agent, or Firm—Pollock, Vande Sande & Priddy

[57] **ABSTRACT**

The invention relates to integrated circuits and, notably, to circuits for which it is desired to provide security against any fraudulent usage. The circuits concerned are microprocessor circuits having a program memory, a programmable non-volatile memory, at least one input/output port and an RS register memorizing the signals from sensors of abnormal conditions. This register is accessible by the microprocessor. There is provision for means to check the state of the register immediately before any operation for the writing or erasure of the programmable memory, and immediately before any transmission of data towards the exterior of the input/output port, and means to interrupt the working of the microprocessor if the check reveals abnormal conditions.

2 Claims, 1 Drawing Sheet



that can be carried out by the microprocessor;

a working random-access memory (RAM) 14;

a non-volatile electrically programmable memory (EPROM) 16 and, preferably, one that is also electrically erasable (EEPROM). This memory may include data and possibly instructions for the microprocessor. It may include, notably, data elements the contents of which should not be touched and confidential data which should not be transmitted to the exterior of the circuit;

input/output ports 18 making it possible, notably, to transmit information on external connection pins I/O of the integrated circuit (the transmission will generally be done serially to minimize the number of pins of the circuit, at least in chip card applications).

Furthermore, the microprocessor is directly connected to registers, the contents of which it can read and which it can reset at zero.

Among these registers, there is an RS register, the inputs of which are connected to various security sensors (C1, C2, C3, C4 for example) such as those mentioned here above.

As has been explained, these sensors are designed to check the environmental conditions and the conditions of operation of the circuit in order to prevent fraudulent operations that would become possible if these conditions were to become abnormal. Examples of sensors have been given here above.

This RS register will be tested according to the invention whenever the program of application of the card (in a ROM or EEPROM memory) involves an operation for the transmission of information to the exterior (by the I/O contact) and also whenever the program involves an operation to modify the contents of the non-volatile memory 16.

These operations are controlled by the microprocessor, by means of sub-programs stored in the read-only memory ROM 12 which manages the entire operation of the card. The organization of the read-only memory 12 is represented symbolically in FIG. 2.

The memory is addressed sequentially, in such a way that the instructions memorized at successive addresses are carried out successively, except for successive instructions for skipping to a different location of the memory.

A starting zone of the memory Z0 contains, for example, an initialization program enabling the microprocessor to carry out preliminary operations after the system is turned on (these preliminary operations include, notably, the zero-setting of the RS register). Preferably, an operation to test the RS register is carried out at the end of the initialization program. At this stage, the conditions of environment and operation of the circuit would indeed have to be normal in order that the circuit may be permitted to function. If the test is positive (with the RS register at zero and no detection of abnormal conditions), then the operation of the integrated circuit continues. If the test is negative (if the register contains a bit relating to the detection of an abnormal condition), then an instruction of routing towards a zone ZF of the ROM is carried out. In this zone ZF, there is placed an instruction or routine placing the microprocessor on standby, and the microprocessor cannot leave this standby state except by reinitialization (for example by being disconnected and turned on again).

Other zones of the program memory 12 are used to carry out various operations. The microprocessor may obtain access to the first address of each of these zones when it receives a command to carry out a certain operation. The zone then contains the series of instructions necessary for the performance of this operation. It is, for example, an application program placed in the EEPROM 16, a program that can be carried out by the microprocessor, which calls up sub-programs placed in the zones of the read-only memory 12 when it has need of them.

Among the possible operations, there is the transmission, to the exterior, of an n-bit word (for example an 8-bit byte) through the input/output port 18. This operation is carried out by means of a sub-program contained in a zone Z1 of the ROM. This sub-program is called upon whenever a word has to be transmitted.

Another operation carried out by a sub-program is the operation for writing a word or a bit in the non-volatile programmable memory 16. The corresponding instructions form a sub-program placed in a zone Z2 of the read-only memory. In the same way, an operation for the erasure of all or part of the programmable memory 16 is carried out by a sub-program placed in a zone Z3 of the read-only memory 12.

According to the invention, it is provided that the first instructions of the zones Z1, Z2 and Z3 will be instructions for checking the state of the RS register, this register being directly accessible in reading mode by the microprocessor. If the result is positive (with normal conditions being detected by the sensors C1 to C4), the sub-program of the zone Z1, Z2 or Z3 respectively is carried out and the corresponding operation (transmission, writing or erasure respectively) is performed. If not, a routing instruction towards the zone ZF is carried out and the microprocessor is placed on definitive standby.

Given the fact that the instructions needed for the checking of the register occupy only some tens of bytes, placed at the start of two or three zones of sub-programs at a maximum, it is seen that the amount of ROM used to provide excellent security is not excessive. This is important, for the available ROM space is limited and should be reserved for numerous other essential operations for the management of the working of the microprocessor.

What is claimed is:

1. An integrated circuit comprising:

a first memory means for storing application programs;

a second memory means which is programmable and non-volatile, for storing data;

at least one I/O port means;

a plurality of means for continually sensing ambient conditions or electrical conditions of the integrated circuit which fall outside a normal operating range;

register means for storing sensing information from the sensing means indicative of said ambient conditions or said electrical conditions of the integrated circuit which fall outside said normal operating range;

a microprocessor means connected to said first and second memory means, said I/O port means, and said register means;

said first memory means storing test subroutines for causing said microprocessor means to detect the presence or absence of said sensing information in said register means only in response to requests for the execution of one or more of said subroutines in the set consisting of;

(a) writing data to said second memory means;

(b) clearing data from said second memory means; or

(c) transmission of data from said second memory means, through the I/O port;

the microprocessor means being interrupted if said sensing information is found to be present in said register means.

2. An integrated circuit as set forth in claim 1 wherein interruption of the microprocessor means causes the microprocessor means to remain in a standby mode until reinitialized.

* * * * *

36/3,K/33 **(Item 33 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014414249 **Image available**
WPI Acc No: 2002-234952/200229
XRPX Acc No: N02-180285

Tamper **proof** integrated circuit **for** smart card **, electronic keys, includes XOR gate that produces reset signal whose state is changed when change occurs in pseudo** random **bit signal of** random **noise** generator

Patent Assignee: SILVERBROOK RES PTY LTD (SILV-N)
Inventor: SILVERBROOK K; WALMSLEY S R
Number of Countries: 001 Number of Patents: 001
Patent Family:

```
Patent No      Kind   Date      Applicat No     Kind   Date       Week
US 6246970      B1   20010612  US 98112761      A    19980710   200229  B
```

Priority Applications (No Type Date): US 98112761 A 19980710
Patent Details:

```
Patent No    Kind Lan Pg   Main IPC     Filing Notes
US 6246970    B1    28 H03K-003/84
```

Tamper **proof** integrated circuit **for** smart card **, electronic keys, includes XOR gate that produces reset signal whose state is changed when change occurs in pseudo** random **bit signal of** random **noise** generator

Abstract (Basic):

... A **random** noise **generator** (1) has an output to provide pseudo random bit signal and another output to provide related signal. The **circuit paths** (2,3) are connected to the corresponding outputs of **random** noise **generator** . An XOR gate (4) which **interconnects** the **circuit paths** , produces a reset signal whose state is changed when change occurs in the bit signal.

... An INDEPENDENT CLAIM is also included for **integrated circuit tamper detection** method...

... **Integrated circuit** (IC) with **tamper detection** circuit for use in **smart card** , authentication chips, electronic keys, cryptographic equipment. Also used in inkjet printer for in-camera digital...

...The **tampering** in the **integrated circuits** is restricted to recover or deduce the key for incorporating security circuits by **testing** the **tampering** in **integrated circuits** using XOR gate. The direct access of top and front sides of the IC is...

...The figure shows the **tampered detection** circuit...

... **Random** noise **generator** (1...

... **Circuit paths** (2,3

Title Terms: **TAMPER** ;

US006246970B1

(12) **United States Patent**
Silverbrook et al.

(10) **Patent No.: US 6,246,970 B1**
(45) **Date of Patent: Jun. 12, 2001**

(54) **METHOD FOR MAKING A CHIP TAMPER-RESISTANT**

(75) Inventors: **Kia Silverbrook; Simon Robert Walmsley**, both of Sydney (AU)

(73) Assignee: **Silverbrook Research Pty Ltd**, Balmain (AU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/112,761**

(22) Filed: **Jul. 10, 1998**

(51) **Int. Cl.^{7}** **H03K 3/84**

(52) **U.S. Cl.** **702/117**; 702/191; 708/256

(58) **Field of Search** 702/117, 189, 702/190, 191; 380/23, 43, 49; 331/78; 708/256

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,153,532 * 10/1992 Albers 331/78

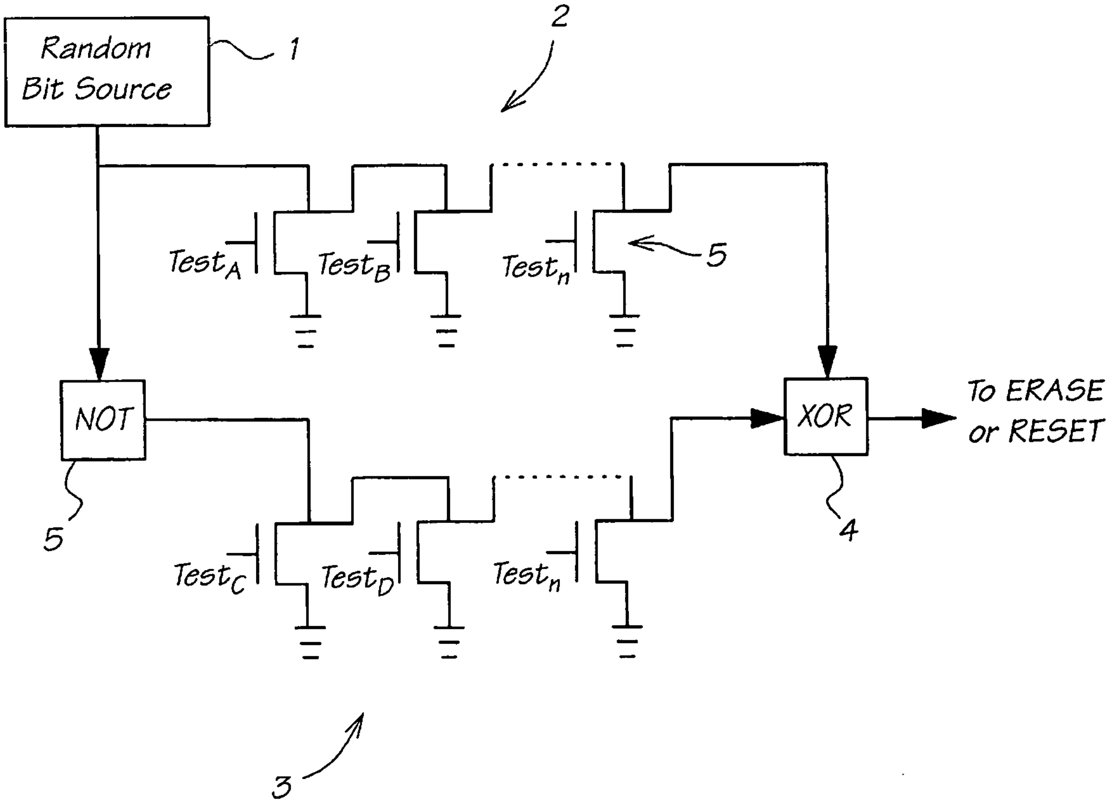
* cited by examiner

Primary Examiner—Kamini Shah

(57) **ABSTRACT**

A method of detecting tampering with an integrated circuit using circuit paths extending in the integrated circuit and carrying signals which are compared to each other, and to thresholds, and providing an output signal in the event that predetermined signal conditions occur. The predetermined signal conditions which occur may be a change of state of an output of a gate which interconnects the two circuit paths, or a change of state of the output of testing circuitry which tests signals in at least one of the circuit paths against a threshold. In a further aspect the invention concerns an integrated circuit chip provided with tamper detecting circuitry.

9 Claims, 5 Drawing Sheets



-continued

INK TYPE

	Description	Advantages	Disadvantages	Examples
	extensively used in offset printing. They have advantages in improved characteristics on paper (especially no wicking or cockle). Oil soluble dies and pigments are required.	medium for some dyes Does not cockle paper Does not wick through paper	this is a significant limitation for use in ink jets, which usually require a low viscosity. Some short chain and multi-branched oils have a sufficiently low viscosity. Slow drying	jets
Micro-emulsion	A microemulsion is a stable, self forming emulsion of oil, water, and surfactant. The characteristic drop size is less than 100 nm, and is determined by the preferred curvature of the surfactant.	Stops ink bleed High dye solubility Water, oil and amphiphilic soluble dies can be used Can stabilize pigment suspensions	Viscosity higher than water Cost is slightly higher than water based ink High surfactant concentration required (around 5%)	All IJ series ink jets

We claim:

1. An integrated circuit including tamper detecting circuitry, comprising: a random noise generator having a first output to provide a first signal comprising a series of pseudo random bits, and a second output to provide a second signal which is related to the first signal, a first circuit path attached to the first output of the random noise generator, and a second circuit path attached to the second output of the random noise generator and at least one gate interconnecting the first and second circuit paths to produce a reset output signal which changes state if tampering causes a change to any bit of the signals in the first and second circuit paths.

2. An integrated circuit according to claim 1 where test circuitry is connected to the first and second circuit paths to test the signals in the paths and provide an output if the signals fall outside a predetermined range.

3. An integrated circuit according to claim 1 where the first and second circuit paths extend through the integrated circuit over the top of circuitry comprising the random noise generator.

4. An integrated circuit according to claim 1 where the second signal is an inverted version of the first signal, and the gate is an exclusive OR gate.

5. A method for detecting tampering with an integrated circuit, comprising the following steps:

providing a random noise generator having a first output to provide a first signal and a second output to provide a second signal, a first circuit path attached to the first output of the random noise generator, and a second circuit path attached to the second output of the random noise generator and at least one gate interconnecting the first and second circuit paths;

generating a series of pseudo random bits in the random noise generator to create a first output string of pseudo random bits at the first output and a second output string of pseudo random bits, related to the first, at the second output;

testing the output of the gate to determine whether there is a change of state.

6. A method according to claim 5, comprising the further step of resetting the integrated circuit in the event of a change of state of the output of the gate.

7. A method according to claim 5, comprising the further step of erasing secret key information in the event of a change of status of the gate.

8. A method according to claim 5, comprising the further step of testing the first and second circuit paths to test the signals in the paths and provide an output if the signals fall outside a predetermined range.

9. A method according to claim 5, where the second signal is an inverted version of the first signal, and the gate is an exclusive OR gate.

* * * * *

```
36/3,K/63     (Item 63 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

009015687     **Image available**
WPI Acc No: 1992-143024/199218
XRPX Acc No: N92-107033
  Increasing protection for  smart   card  carrying  memory  - uses random
  time interval between receipt of signal by card and return of card
  response, to prevent fraudulent use of time delay of find code
Patent Assignee: GERONIMI F (GERO-I); GEMPLUS CARD INT SA (GEMP-N)
Inventor: GERONIMI F; LISIMAQUE G; LISMAQUE G
Number of Countries: 009  Number of Patents: 009
Patent Family:
Patent No     Kind   Date     Applicat No    Kind   Date     Week
EP 482975      A   19920429  EP 91402637     A   19911003  199218  B
FR 2667715     A1  19920410  FR 9012440      A   19901009  199222
CA 2053001     A   19920410  CA 2053001      A   19911008  199226
EP 482975      B1  19931222  EP 91402637     A   19911003  199351
DE 69100836    E   19940203  DE 600836       A   19911003  199406
                             EP 91402637     A   19911003
ES 2065646     T3  19950216  EP 91402637     A   19911003  199513
US 5477039     A   19951219  US 91773448     A   19911009  199605
                             US 93165869     A   19931214
CA 2053001     C   19960220  CA 2053001      A   19911008  199618
JP 3155973     B2  20010416  JP 91290520     A   19911009  200124

Priority Applications (No Type Date): FR 9012440 A 19901009
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
EP 482975     A  F   7
   Designated States (Regional): DE ES GB IT NL
FR 2667715    A1      G06K-019/073
CA 2053001    A  F    G06K-019/073
EP 482975     B1 F   8 G06K-019/06
   Designated States (Regional): DE ES GB IT NL
DE 69100836   E       G06K-019/06   Based on patent EP 482975
ES 2065646    T3      G06K-019/06   Based on patent EP 482975
US 5477039    A      6 G06K-005/00   Cont of application US 91773448
CA 2053001    C  F    G06K-019/073
JP 3155973    B2     4 G06K-019/073  Previous Publ. patent JP 4263384

  Increasing protection for  smart   card  carrying  memory  -

...Abstract (Basic): The protection is applied to cards carrying  memory
    and also a microcircuit having  memory  coupled to the data  processing
     element. When the  processor  is activated by an external data signal
    it emits a ratification signal after a randomly...

...After data entry (1) a  random  number is  generated  (2) and used to
    set a time counter (3). At the end of the count...
...Abstract (Equivalent): A method to increase the protection of a
    microcircuit-based  memory  card comprising at least one  memory  (13,
    14) coupled to a data- processing  element (15) wherein, said data-
    processing  element receiving a command by a data signal external to
    the card and emitting in...
...Abstract (Equivalent): A  memory  card, said  memory  card comprising...

...a bus, said bus permitting communication between an external device and
    said  memory  card...
```

...a first **memory** , said first **memory** being coupled to said bus, and said first **memory** having an application program stored therein...

...a second **memory** , said second **memory** being coupled to said bus...

...a circuit for **generating** a **random** delay value, said circuit being coupled to said bus; and...

...a **processing** element, said **processing** element being coupled to said bus, and said **processing** element defining means...

...for transmitting **data** **via** said bus to said second **memory** for storage therein...

...for delaying transmission of an end-of-control signal from said **memory** card to said external device by an amount of time proportional to said random delay...
...Title Terms: **MEMORY** ;

US005477039A

United States Patent [19]

Lisimaque et al.

[11] **Patent Number: 5,477,039**

[45] **Date of Patent: Dec. 19, 1995**

[54] **METHOD AND DEVICE TO INCREASE THE PROTECTION OF A CHIP CARD**

[75] Inventors: **Gilles Lisimaque**, Potomac, Md.; **François Geronimi**, Aix En Provence, France

[73] Assignee: **Gemplus Card International**, Gemenos, France

[21] Appl. No.: **165,869**

[22] Filed: **Dec. 14, 1993**

Related U.S. Application Data

[63] Continuation of Ser. No. 773,448, Oct. 9, 1991, abandoned.

[30] **Foreign Application Priority Data**

Oct. 9, 1990 [FR] France 90 12440

[51] **Int. Cl.**^{6} **G06K 5/00**; G06K 19/06

[52] **U.S. Cl.** **235/380**; 235/382; 235/492

[58] **Field of Search** 235/492, 493, 235/494, 380, 382, 382.5

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,471,216	9/1984	Herve	235/380
4,870,574	9/1989	Lisisimaque	364/300

FOREIGN PATENT DOCUMENTS

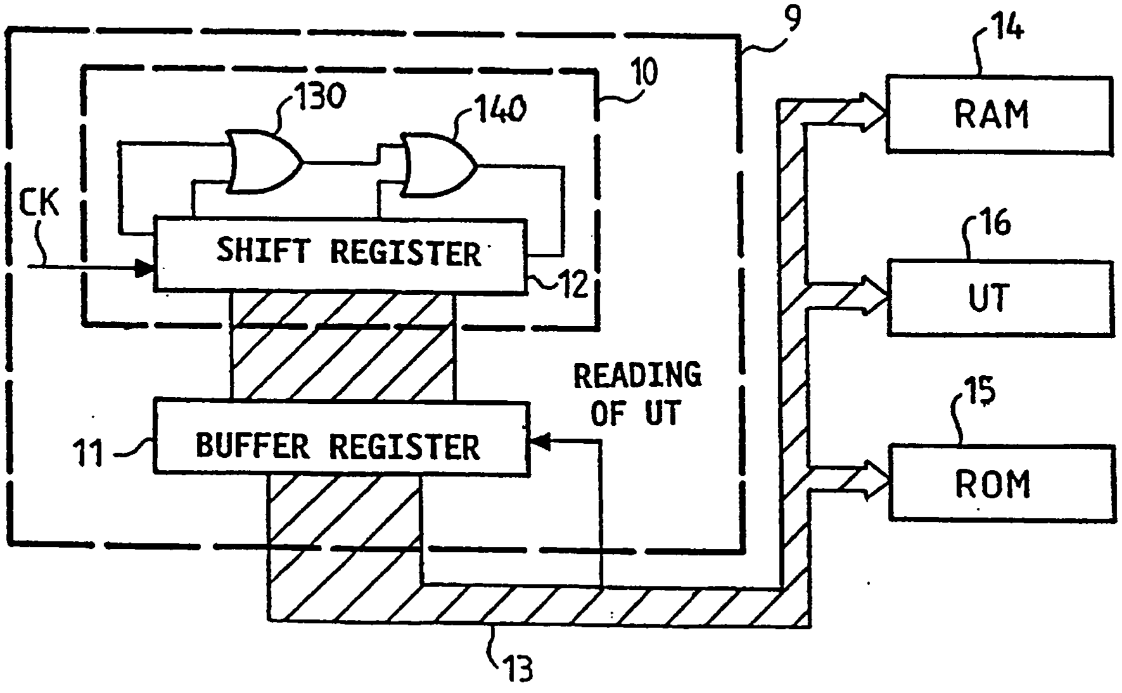
0243873	11/1987	European Pat. Off. .
0314148	5/1989	European Pat. Off. .
8802899	4/1988	WIPO .

Primary Examiner—Timothy P. Callahan
Assistant Examiner—Trong Phan
Attorney, Agent, or Firm—Nilles & Nilles

[57] **ABSTRACT**

The method is designed to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element. When said data-processing element receives a command by a data signal external to the card, said method consists in making said data-processing element emit a ratification signal at an instant that is deferred, with respect to the instant at which its emission was prompted by the data signal, by a duration that is randomly variable in time. The disclosed method can be applied to microcircuit-based memory cards.

8 Claims, 2 Drawing Sheets



of the memory card. At steps 2 and 3 respectively, a random number A is drawn and pulses given continuously by a fixed clock (not shown) are counted in known way. Simultaneously, a program corresponding to the data and/or to the corresponding command is launched at step 4 to carry out operations for writing, reading the memory of the card and/or for example computing a signature. At the end of the execution of these instructions, the program emits an end-of-control signal or acknowledgment signal at step 5. At step 6, a comparison is made between the random number drawn at step 2 and the count made at step 3. When the number indicated by the count at step 3 is equal to the random number obtained at step 6, the end-of-control signal emitted at step 5 is validated at step 7. Then, at step 8, this signal is sent out of the card into a card reading/writing device (not shown). In this way, as can be seen in the diagram of FIG. 2, whenever a data element or command is sent to the card, the card can emit an end-of-control or acknowledgment signal CR acknowledging receipt of the data and commands that it has received after a period of time T. The duration of this time T, which is always random, can never provide information on the particular type of function that the card has been made to perform.

Naturally, the mode of execution of the method just described is not the only possible one, and other variants are possible by modifying, for example, the order or the content of steps 1 to 8, as can be seen in FIG. 3 where elements homologous to those of FIG. 1 are shown with the same references. In FIG. 3, the drawing of the random number A takes place at the step 2, not as in FIG. 1 as soon as the execution of the data input step 1 has ended but during or at the end of execution of the control program at step 4. Furthermore, the initialization of the counting at step 3 takes place not as soon as the execution of step 1 has ended but when the random number A has been drawn at the step 2. As in FIG. 1, incrementation of the counting at step 3 takes place for as long as the counting at step 6 has not reached the value of the random number A.

An embodiment of a circuit 19 for the implementation of the above method and its interconnection with the elements forming a memory card are shown in FIG. 4. The circuit 19 has a random code generator shown within a box of dashed lines 10. The parallel outputs of the generator 10 are connected to the parallel inputs of a buffer register 11. In the example of FIG. 4, the random code generator has, in a known way, a shift register 12 with outputs looped to inputs through exclusive-OR circuits 130, 140.

The connection of the circuit 19 to the other elements which, in a standard way, form a memory card, is done by means of the data bus 13 of these cards which connect RAM type memories 14 and ROM or EPROM type memories 15 to their processing unit 16. The connection to the data bus 13 takes place through the outputs of the buffer register 11.

To execute the method according to the invention, the shift register 12 is preferably controlled at the rate of a clock signal CK which is different from the clock signal used to determine the processing cycles of the processing unit 16. When, as shown in FIG. 3, the processing unit 16 carries out the control program 4 to draw the random number A, a reading signal UT of the processing unit 16 is applied to a control input of the buffer register 11 to hold the drawn random number A in the register and provide for its transfer to the bus 13. It must be noted that, according to this approach, the clock signal CK may be made variable, notably as a function of the temperature and of the supply voltages of the card so as to also have a random character.

Naturally, the embodiment of the circuit 19 that has just

been described is not the only possible one. If necessary, a purely logic type embodiment may be preferred, with the implementation of a logic exclusive-OR function XOR as represented schematically in FIG. 5 by an equivalent exclusive OR gate 19. The output of the exclusive OR gate is looped to a first input, and the second input receives for example the value of the data transmitted to the card, all or a part of the data and instructions contained in the RAM 14, and the contents of all or a part of the ROM 15.

It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements.

What is claimed is:

1. A memory card, said memory card comprising:

a bus, said bus permitting communication between an external device and said memory card;

a first memory, said first memory being coupled to said bus, and said first memory having an application program stored therein;

a second memory, said second memory being coupled to said bus;

a circuit for generating a random delay value, said circuit being coupled to said bus; and

a processing element, said processing element being coupled to said bus, and said processing element defining means

for receiving instructions from said application program via said bus,

for executing said application program instructions,

for transmitting data via said bus to said second memory for storage therein,

for receiving said random delay value via said bus, and

for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value.

2. The memory card as in claim 1, wherein said random number circuit further comprises:

a random code generator, said random code generator including

a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and

a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and

a buffer register, said buffer register connecting said random code generator to said bus.

3. The memory card as in claim 1, wherein said first memory is read only memory and wherein said second memory is random access memory.

4. The memory card as in claim 1, wherein said first memory is volatile memory, and wherein said second memory is nonvolatile memory.

5. A method to increase the security of a micro-circuit based chip card having a memory, and a data processing element receiving a data signal command from an external device, the method comprising the steps of:

generating a random delay value following receipt of said data signal command;

triggering a delay count to initiate a time interval;

generating an end-of-control signal;

incrementing said delay count;

comparing said random delay value to said delay count; and

transmitting said end-of-control signal when said delay count is equal to said random delay value.

6. The method set forth in claim 5 wherein the randomly generated value is generated by random code generation.

7. The method as in claim 5, wherein said triggering step

occurs after said data processing element receives said data signal command from said external device, and wherein said triggering step occurs before said generating step.

8. The method as in claim 5, wherein said triggering step occurs after said generating step and before said incrementing step.

* * * * *

36/3,K/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010618896 **Image available**
WPI Acc No: 1996-115849/199612
XRPX Acc No: N96-096913

Integrated circuit card **for** memory **card - has switch connecting power supply lines based on** detection **result of voltage** detector **and connecting host power supply line to main circuit supply line when absolute value of host voltage is less than prescribed voltage**

Patent Assignee: SEIKO EPSON CORP (SHIH)
Inventor: ODA Z; SAKURADA N
Number of Countries: 002 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5490117	A	19960206	US 94216272	A	19940323	199612	B
JP 2003308502	A	20031031	JP 93353820	A	19931228	200374	
			JP 2003119642	A	19931228		
JP 3477781	B2	20031210	JP 93353820	A	19931228	200382	
JP 3562524	B2	20040908	JP 93353820	A	19931228	200459	
			JP 2003119642	A	19931228		

Priority Applications (No Type Date): JP 93353820 A 19931228; JP 9364347 A 19930323

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5490117	A		29	G11C-013/00	
JP 2003308502	A		18	G06K-019/07	Div ex application JP 93353820
JP 3477781	B2		22	G06K-019/07	Previous Publ. patent JP 6333103
JP 3562524	B2		24	G06K-019/07	Div ex application JP 93353820
					Previous Publ. patent JP 2003308502

Integrated circuit card **for** memory **card...**

...**has switch connecting power supply lines based on** detection **result of voltage** detector **and connecting host power supply line to main circuit supply line when absolute value of...**

...Abstract (Basic): The **IC card** comprises a main circuit, a **connector** for connecting the **IC card** to a host system and an interface circuit between the **connector** and the main circuit. The interface circuit comprises an external interface circuit for connecting the...

...interface circuit is connected to a power supply line of the main circuit. A voltage **detecting** device for **detects** a voltage of the host system power supply line...

...A switching device for selectively connects and **disconnects** the host system power supply line and the main circuit power supply line based on a **detection** result of the voltage **detection** device. The switching device connects the host system power supply line to the main circuit...

...supply line is less than an absolute value of a prescribed voltage. The switching device **disconnects** the host power supply line from the main circuit power supply line when the absolute...

...USE/ADVANTAGE - For SRAM, DRAM, mask **ROM** , **EPROM** , OTPROM, **EPROM** and flash **EEPROM** cards. Has one-chip configuration. Reduces power

```
    consumption...
...Title Terms:  **MEMORY** ;
```

US005490117A

United States Patent [19]

Oda et al.

[11] **Patent Number: 5,490,117**

[45] **Date of Patent: Feb. 6, 1996**

[54] **IC CARD WITH DUAL LEVEL POWER SUPPLY INTERFACE AND METHOD FOR OPERATING THE IC CARD**

[75] Inventors: **Zenzo Oda; Noriaki Sakurada**, both of Suwa, Japan

[73] Assignee: **Seiko Epson Corporation**, Tokyo, Japan

[21] Appl. No.: **216,272**

[22] Filed: **Mar. 23, 1994**

[30] **Foreign Application Priority Data**

Mar. 23, 1993	[JP]	Japan	5-064347
Dec. 28, 1993	[JP]	Japan	5-353820

[51] **Int. Cl.⁶** **G11C 13/00**; G11C 14/00

[52] **U.S. Cl.** **365/226**; 365/189.01; 365/228; 365/229

[58] **Field of Search** 365/226, 227, 365/228, 229, 189.01; 235/492

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,016,223	5/1991	Kimura	365/229
5,138,142	8/1992	Sanemitsu	235/492
5,245,582	9/1993	Kimura	365/229
5,329,491	7/1994	Brown	365/226

FOREIGN PATENT DOCUMENTS

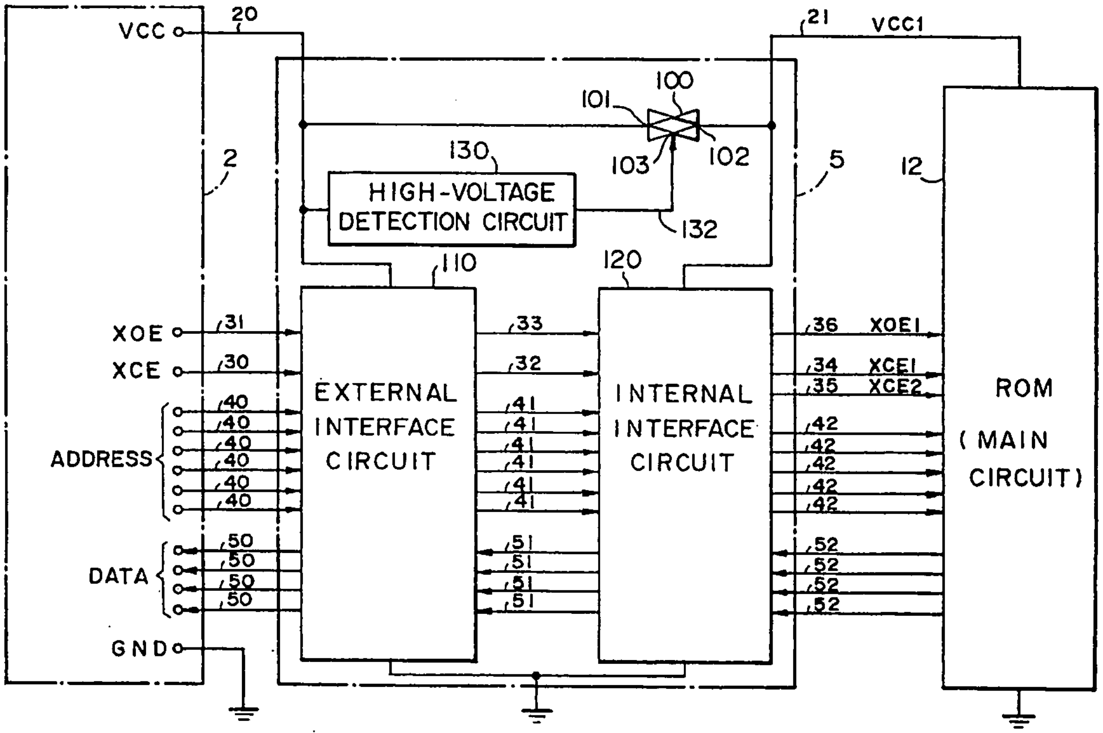
2-259853	10/1990	Japan .
4-30208	2/1992	Japan .

Primary Examiner—David C. Nelms
Assistant Examiner—Son Mai
Attorney, Agent, or Firm—Oliff & Berridge

[57] **ABSTRACT**

An objective of the present invention is to provide a highly reliable IC card which is large in the scale of integration, fast, and low power-consuming, which contains the latest type of IC that has an operating voltage of 3.3 V and a maximum rated voltage of 5 V or less, and which can be used in either the latest equipment rated at 3.3 V or existing equipment rated at 5 V, or which does not cause this latest type of IC to be destroyed. The interface circuit comprises an analog switch, an external interface circuit, an interval interface circuit, and a high-voltage detection circuit. If the voltage of the power supply Vcc of the host system is less than or equal to an upper-limit voltage of 4 V, the power supply voltage is applied unchanged through the analog switch to a ROM that is the main circuit. On the other hand, if the power supply voltage is greater than this upper-limit voltage of 4 V, the analog switch is made non-conductive and thus the power supply voltage is not applied to the ROM. This prevents the ROM from being destroyed. If a regulated-voltage circuit is also provided, a power supply voltage regulated at 3.3 V can be applied to the ROM, even when the power supply voltage of host system is greater than the upper-limit voltage of 4 V.

36 Claims, 15 Drawing Sheets



36/3,K/47 (Item 47 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012570508 **Image available**
WPI Acc No: 1999-376615/199932
XRPX Acc No: N99-281642

Information transfer controller of card-like memory **medium such as** integrated circuit card **inserted in personal computer - controls to** stop **transfer of information and to maintain information in** memory **,** **when lock releasing condition is** detected **by lock** detector

```
Patent Assignee: OKI ELECTRIC IND CO LTD (OKID  )
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind    Date     Applicat No     Kind    Date      Week
JP 11144005     A    19990528  JP 97310140      A    19971112  199932  B

Priority Applications (No Type Date): JP 97310140 A 19971112
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
JP 11144005   A      7 G06K-017/00
```

Information transfer controller of card-like memory **medium such as** integrated circuit card **inserted in personal computer...**
...**controls to** stop **transfer of information and to maintain information in** memory , **when lock releasing condition is** detected **by lock** detector

...Abstract (Basic): NOVELTY - A control unit controls transfer of information on an **IC card** (1) to a **memory** , when lock condition of a door (5) is **detected** by a lock **detector** (17). The control unit controls to **stop** transfer of information and to maintain information in the **memory** , when lock releasing condition is **detected** . DETAILED DESCRIPTION - A card mounting stand (4) has the door (5), a **connector** and the card **detector** . The **connector** is connected with a contact of an **IC card** (1), when the card is inserted in the stand and the door is closed. A...

...is seeped into a long hole of the door, for locking the door. A lock **detector** (17) **detects** lock condition of the door...

...USE - For controlling information transfer between **integrated circuit card** and personal computer...

...of card, reliably. DESCRIPTION OF DRAWING(S) - The figure depicts the perspective view of information **processor** . (1) **IC card** ; (4) Card mounting stand; (5) Door; (13) Lock; (14) Lever; (17) Lock **detector** .

...Title Terms: **MEMORY** ;

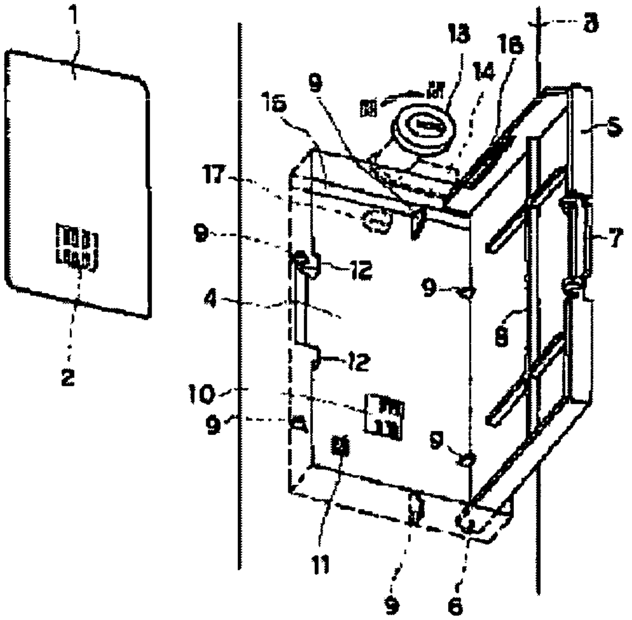
INFORMATION PROCESSOR

Patent number:	JP11144005
Publication date:	1999-05-28
Inventor:	SUGIMOTO YASUKI
Applicant:	OKI ELECTRIC IND CO LTD
Classification:	
- international:	G06K17/00; G06F1/16; G06F12/16
- european:	
Application number:	JP19970310140 19971112
Priority number(s):	JP19970310140 19971112

Report a data error here

Abstract of **JP11144005**

PROBLEM TO BE SOLVED: To protect information if a door is to be opened by mistake during the transfer of the information to a card type storage medium. SOLUTION: When the card type storage medium 1 is inserted into a medium loading part 4 and the door 5 is closed, the loading of the card type storage medium 1 is detected and when a lock 13 is rotated with a key, a rotary lever 14 enters a long hole 16 bored in the door 5 together with the lock 13; and a lock detecting means 17 detects the locked state of the door 5 once the door 5 is locked. In this state, the transmission and reception of information to and from the card type storage medium 1 are made possible and when the signal of the lock detecting means 17 changes from the locked state to an unlocked state, a control part performs control so that the transmission and reception of the information are quit and the information is held in a memory.



Data supplied from the ***esp@cenet*** database - Worldwide

36/3,K/57 (Item 57 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010403751 **Image available**
WPI Acc No: 1995-305065/199540

IC card processing **device for** memory **circuit -** detects **status of connections of card with** conductor **with external terminals**

Patent Assignee: ANRITSU CORP (ANRI)
Inventor: MUTO N; TAKA K
Number of Countries: 003 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 7200757	A	19950804	JP 93350388	A	19931231	199540	B
US 5478996	A	19951226	US 94310653	A	19940922	199606	
MX 188122	B	19980227	MX 947513	A	19940929	200045	

Priority Applications (No Type Date): JP 93350388 A 19931231
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 7200757	A		9	G06K-017/00	
US 5478996	A		13	G06K-007/06	
MX 188122	B			G06K-007/006	

IC card processing **device for** memory **circuit...**
... detects **status of connections of card with** conductor **with external terminals**

...Abstract (Basic): The **IC card processing** device has a **conductor** (5) connecting card (3) to the required terminal. External terminal (4) in touch with a contact terminal when **electrical connection** is being routed to the card. A control circuit (51) **monitors** the communication between the contact terminal and a receiver (45), when radio wave signals from a clock signal source (CL1) to pass to the **conductor** .

...

...card which has been inserted into the accommodating unit, an electrical signal is sent to **detection** circuit (46) in the control circuit. A switch (44) is actuated during **detection** and remains open until the **detection** is completed. The signal status being judged by the **detection** circuit provides information on the instructed card position
...Abstract (Equivalent): An **IC card processing** apparatus comprising ...

...an insertion port for receiving an **IC card** having an external terminal...
...an **IC card** storage unit for storing said **IC card** inserted from said insertion port...

...a contact terminal to be brought into contact with said external terminal of said **IC card** inserted from said insertion port...

... **detection** means for **detecting** that said **IC card** is inserted from said insertion port to a predetermined position of said **IC card** storage unit...

...an information **processing** circuit for exchanging information with said external terminal through said contact terminal; and...

...wrong card **detection** means, having a terminal capable of being brought into contact with said contact terminal, for **detecting** that a wrong card including a conductive line extending from said terminal is inserted from...

...said wrong card **detection** means comprising...

...a) switch means, arranged near said contact terminal, for **disconnecting** a connection between said contact terminal and said information **processing** circuit in response to a **detection** signal from said **detecting** means...

...b) a reception circuit for **detecting** an electric field strength appearing at said contact terminal when the connection between said contact terminal and said information **processing** circuit is **disconnected** by said switch means...

...c) a determination circuit for receiving an output from said reception circuit to **check** whether the electric field strength exceeds a predetermined value; and...

...determination circuit is completed, said switch means to connect said contact terminal to said information **processing** circuit
...Title Terms: **MEMORY** ;

US005478996A

United States Patent [19]

Muto et al.

[11] **Patent Number: 5,478,996**

[45] **Date of Patent: Dec. 26, 1995**

[54] **IC CARD PROCESSING APPARATUS HAVING FUNCTION FOR DETECTING AND PROTECTING DISHONEST UTILIZATION USING SWITCH MEANS**

[75] Inventors: **Norikazu Muto; Katsuhiro Taka**, both of Atsugi, Japan

[73] Assignee: **Anritsu Corporation**, Tokyo, Japan

[21] Appl. No.: **310,653**

[22] Filed: **Sep. 22, 1994**

[30] **Foreign Application Priority Data**

Dec. 31, 1993 [JP] Japan 5-350388

[51] **Int. Cl.**^{6} **G06K 7/06**

[52] **U.S. Cl.** **235/441**

[58] **Field of Search** 235/441, 439; 307/112, 116, 117; 340/825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,999,601	3/1991	Gervais	235/492

FOREIGN PATENT DOCUMENTS

2554262	3/1985	France .

Primary Examiner—John Shepperd

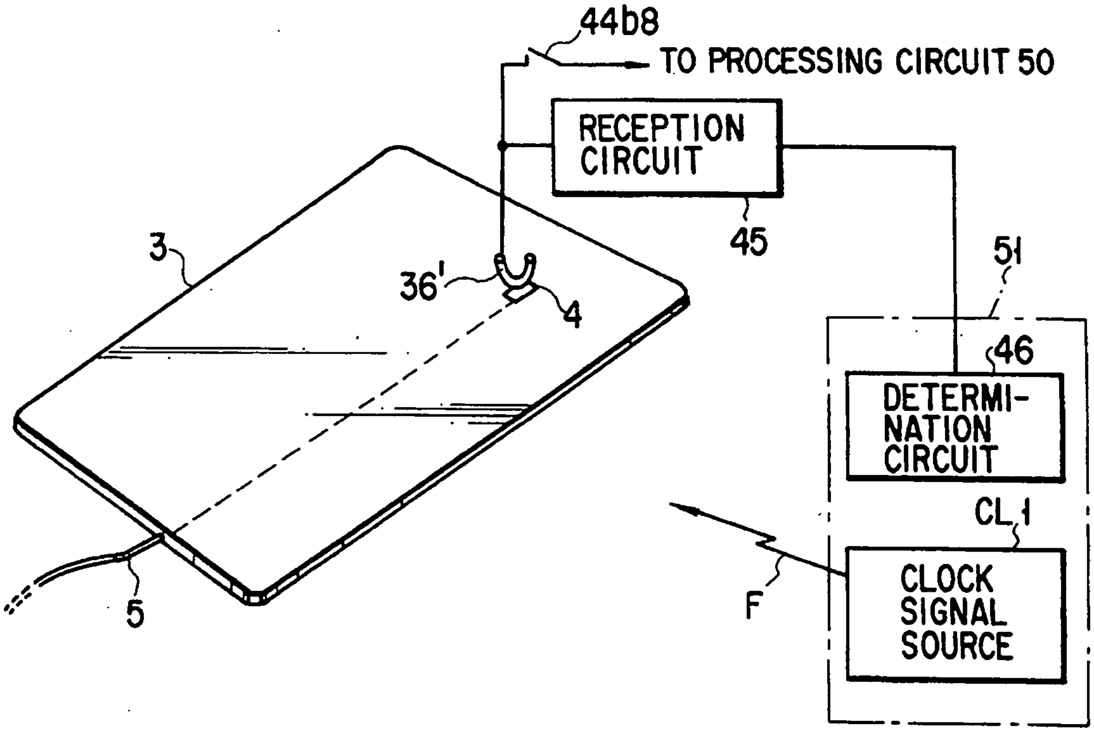
Assistant Examiner—Michael G. Lee

Attorney, Agent, or Firm—Frishauf, Holtz, Goodman, Langer & Chick

[57] **ABSTRACT**

In order to enable a processing circuit to certainly detect insertion of a wrong card having a conductive line without using a plate member or a coil regulating the shape of a card storage unit, when the wrong card having the conductive line is inserted from a card insertion port, formed in one surface of a housing, into the card storage unit in the housing, and the external terminal of the card is brought into contact with a contact terminal, a radio wave radiated into the housing is induced to the conductive line. A reception circuit connected to the contact terminal receives, of signals appearing at the conductive line, a radio wave signal radiated from a clock signal source in a communication control unit located at a position spaced apart from the card storage unit and supplies the detection output of the radio wave signal to a determination circuit. The determination circuit determines insertion of the wrong card having the conductive line on the basis of the detection output. During this determination operation, a switch element is set in an open state, and the contact terminal is disconnected from the processing circuit, so that the voltage induced to the conductive line of the wrong card and the voltage induced to the external terminal of a proper card can be taken a sufficient value to determine the difference therebetween.

12 Claims, 6 Drawing Sheets



connecting the input/output terminals of an inverter **60***a* to each other by a quartz oscillator **60***b* and connecting capacitors **60***c* and **60***d* to both the terminals of the quartz oscillator **60***b*, a radio wave having the frequency F and output from the clock signal source **60** is strongly radiated. For this reason, the level of a signal input to the reception circuit **45** increases, and the presence/absence of the conductive line of the card can be determined at a high S/N ratio.

According to the above embodiment, in order to receive a very weak radio wave, the superheterodyne reception circuit **45** is used. However, if strong radio waves are radiated from high-frequency signal sources, a reception circuit can be constituted by only a filter and a detector, or an amplifier in addition to the filter and the detector. In this case, the amplifier may be connected to the input terminal of the filter or between the filter and the detector. In addition, in an apparatus which includes only one high-frequency signal source, a filter can be omitted.

In the embodiment, although the determination circuit **46** is arranged in the communication control unit **51** separated from the mechanism unit **21**, the determination circuit **46** may be arranged on the circuit board **40** on the mechanism unit **21** side.

In the embodiment, although the switch elements **44b1** to **44b8** of the relay **44** are used as switch elements, a semiconductor switch (e.g., an analog switch, a gate switch, or a photocoupler) or a filter circuit capable of performing signal separation for a high-frequency signal may be used in place of the relay **44**.

In the embodiment, although an output from the reception circuit **45** is used only to detect the conductive line of a wrong card, it may be checked on the basis of this reception output whether the detection circuit is entirely normally operated.

In the embodiment, a manual insertion type IC card processing apparatus has been described. However, the present invention can be similarly applied to a card processing apparatus in which an IC card inserted from a card insertion port is completely received into a card storage unit.

As described above, in an IC card processing apparatus according to the present invention, a radio wave radiated from a high-frequency signal source of an electronic circuit located at a position separated from a card storage unit is induced to the conductive line of a wrong card received into the card storage unit, and a signal appearing at a contact terminal which is in contact with an external terminal of the card connected to the conductive line is received, thereby determining, on the basis of the reception output, that the inserted card is a wrong card.

As described above, according to the present invention, since the conductive line of a wrong card is used as reception antenna for receiving a radio wave radiated into the housing, the diameter and the position of the conductive line rarely affect a reception output, and the wrong card can be certainly detected.

According to the present invention, unlike the prior art, a conductive plate for capacitively coupling the conductive line of a wrong card, a plate for emitting an electromagnetic wave, and the like need not be arranged between the card insertion port and the contact terminals. For this reason, the shape of the card storage unit is not limited, and a large opening can be formed in the lower surface of the card storage unit, thereby preventing a card jam caused by insertion of a card cut shorter than a proper card, a piece of paper, or the like.

Additional embodiments of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the present invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with the true scope of the present invention being indicated by following claims.

What is claimed is:

1. An IC card processing apparatus comprising:

an insertion port for receiving an IC card having an external terminal;

an IC card storage unit for storing said IC card inserted from said insertion port;

a contact terminal to be brought into contact with said external terminal of said IC card inserted from said insertion port;

detection means for detecting that said IC card is inserted from said insertion port to a predetermined position of said IC card storage unit;

an information processing circuit for exchanging information with said external terminal through said contact terminal; and

wrong card detection means, having a terminal capable of being brought into contact with said contact terminal, for detecting that a wrong card including a conductive line extending from said terminal is inserted from said insertion port,

said wrong card detection means comprising:

a) switch means, arranged near said contact terminal, for disconnecting a connection between said contact terminal and said information processing circuit in response to a detection signal from said detecting means;

b) a reception circuit for detecting an electric field strength appearing at said contact terminal when the connection between said contact terminal and said information processing circuit is disconnected by said switch means;

c) a determination circuit for receiving an output from said reception circuit to check whether the electric field strength exceeds a predetermined value; and

d) switch control means for switching, when the determination of said determination circuit is completed, said switch means to connect said contact terminal to said information processing circuit.

2. An apparatus according to claim **1**, wherein said switch means includes a relay contact.

3. An apparatus according to claim **1**, wherein the electric field includes a high-frequency component leaking and radiated from a specific clock signal source used in said information processing circuit.

4. An apparatus according to claim **1**, wherein a large opening is formed in a lower surface of said IC card storage unit to cause the IC card storage unit to drop a card cut shorter than a proper IC card, dust, and the like downward.

5. An apparatus according to claim **3**, wherein said reception circuit includes a superheterodyne reception circuit for detecting that a high-frequency component radiated from said specific clock signal source appears at said connection terminal.

6. An apparatus according to claim **1**, wherein said contact terminal is connected to said reception circuit with a shortest distance.

7. An apparatus according to claim **1**, wherein, when said contact terminal comprises a plurality of contact terminals, said switch means includes a plurality of switches for respectively disconnecting connections between said plurality of contact terminals and said information processing circuit.

8. An apparatus according to claim 1, wherein said determination circuit uses a reference voltage which is preset to be higher than an output, obtained from said reception circuit when a proper card is inserted, by a voltage corresponding to a predetermined margin and to be lower than an output obtained from said reception circuit when a conductive line having a predetermined length is connected to said contact terminal.

9. An apparatus according to claim 1, further comprising:

power supply control means for supplying power to said reception circuit in response to a detection signal from said detection means and stopping power supply to said reception circuit in response to a determination completion of said determination circuit.

10. An apparatus according to claim 1, wherein said apparatus is accommodated in a housing shielded electromagnetically.

11. An apparatus according to claim 10, further comprising:

radio wave radiation means including a dedicated clock signal source to the electric field and an antenna for radiating a radio wave from said dedicated clock signal source into said housing.

12. An apparatus according to claim 1, wherein said IC card includes a prepaid IC memory card which stores call rate information for a public telephone set.

* * * * *

```
36/3,K/5     (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

009660287     **Image available**
WPI Acc No: 1993-353838/199345
XRPX Acc No: N93-272958
  I-O control circuit for  integrated   circuit   card  with one-time  PROM
    ICs - includes selection circuit to detect  PROM  power supply voltage
  and select one of read or write  data   bus  buffers, both connected
  between  PROM  ICs and  data   bus , with either 5V read or 12-12.5V
  program supply voltage, respectively
Patent Assignee: MITSUBISHI DENKI KK (MITQ  )
Inventor: GOCHI H
Number of Countries: 003  Number of Patents: 005
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
GB 2267164     A   19931124  GB 938801       A   19930428  199345  B
DE 4316894     A1  19931202  DE 4316894      A   19930519  199349
US 5378944     A   19950103  US 9359935      A   19930511  199507
GB 2267164     B   19951011  GB 938801       A   19930428  199544
DE 4316894     C2  19951019  DE 4316894      A   19930519  199546

Priority Applications (No Type Date): JP 92127483 A 19920520
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
GB 2267164    A     19 G11C-007/00
DE 4316894    A1    10 G06K-007/00
US 5378944    A      8 H03K-019/0175
GB 2267164    B      2 G11C-007/00
DE 4316894    C2     9 G06K-007/00

  I-O control circuit for  integrated   circuit   card  with one-time  PROM
    ICs...

...includes selection circuit to detect  PROM  power supply voltage and
  select one of read or write  data   bus  buffers, both connected between
  PROM  ICs and  data   bus , with either 5V read or 12-12.5V program
  supply voltage, respectively

...Abstract (Basic): The  IC   card  input-output control circuit has a
    read  data   bus  buffer (35) connected between the one-time  PROM  ICs
    (21) and a  data   bus  (29) and a write  data   bus  buffer (36)
    connected between the  PROM  ICs and the  data   bus . Selection
    circuitry (37)  detects  the power supply voltage supplied to the  PROM
     ICs and selects either the read or write  data   bus  buffer
    accordingly...
...a Zener diode and resistance series connected between a power supply
    voltage line to the  PROM  IC and ground. One of the  PROM  ICs in the
    IC   card  is selected by an address decoder in response to an address
    signal...

...ADVANTAGE - Increased resistance to static electricity;  IC   card
    electrical characteristics esp. output terminal capacity independent of
    number of  PROMs  mounted on card...
...Abstract (Equivalent): an input/output circuit for a I.C. card which is
    provided with a PRIM  integrated   circuit , programmable only once...
...Abstract (Equivalent): An input/output control circuit for an  IC   card
     equipped with one-time PROMICs, comprising...
```

...a read **data bus** buffer connected between said one-time PROMICs and a **data bus** :

...

...a write **data bus** buffer connected between said one-time PROMICs and the said **data bus** ; and...

...power supply voltage supplied to said one-time PROMICs and selecting one of said read **data bus** buffer and said write **data bus** buffer on the basis of the **detected** power supply voltage

...Abstract (Equivalent): The input/output control circuit for an **IC card** equipped with one-time programmable read only **memory integrated circuits** (**PROM** -ICs) includes a read **data bus** buffer connected between the one-time **PROM** -ICs and a **data bus**0 . A write **data bus** buffer is connected between the one time **PROM** -ICs and the **data bus** .

...

...A selection device detects the power supply voltage supplied to the one-time **PROM** -ICs and selects one of the read **data bus** buffer and the write **data bus** buffer in response to the **detected** power supply voltage...

...ADVANTAGE - input/output control circuit improves ability of **IC card** to withstand electrostatic discharge and prevents electrical characteristics of **IC card** from changing with change in number of one-time **PROM** -ICs mounted on it

...Title Terms: **PROM** ;

US005378944A

United States Patent [19]

Gochi

[11] **Patent Number: 5,378,944**

[45] **Date of Patent: Jan. 3, 1995**

[54] **IC CARD INPUT/OUTPUT CONTROL CIRCUIT**

[75] Inventor: **Hidenobu Gochi**, Itami, Japan

[73] Assignee: **Mitsubishi Denki Kabushiki Kaisha**, Tokyo, Japan

[21] Appl. No.: **59,935**

[22] Filed: **May 11, 1993**

[30] **Foreign Application Priority Data**

May 20, 1992 [JP] Japan 4-127483

[51] **Int. Cl.⁶** **H03K 19/0175; H03K 17/16**

[52] **U.S. Cl.** **326/62**; 365/206; 365/52; 365/189.05; 326/21; 326/105

[58] **Field of Search** 307/465, 443, 475; 365/206, 52, 189.05

[56] **References Cited**

U.S. PATENT DOCUMENTS

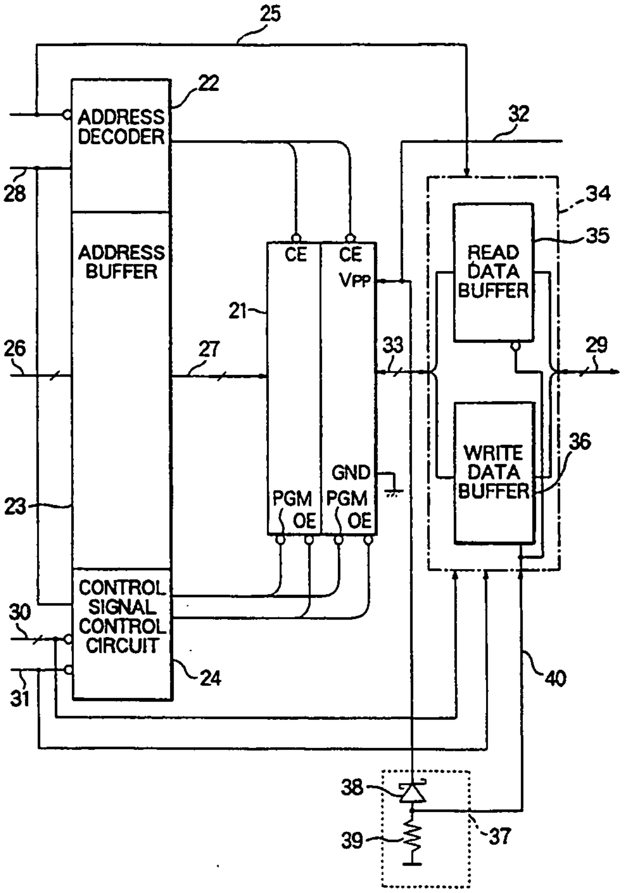
4,498,022	2/1985	Koyama et al.	307/473
4,916,662	4/1990	Mizuta	365/52
5,016,223	5/1991	Kimura et al.	365/52
5,025,415	6/1991	Masuyama et al.	365/52
5,202,852	4/1993	Mizuta	365/189.05
5,241,662	8/1993	Maniwa et al.	395/425

Primary Examiner—Edward P. Westin
Assistant Examiner—Richard Roseen
Attorney, Agent, or Firm—Leydig, Voit & Mayer

[57] **ABSTRACT**

An input/output control circuit for an IC card equipped with one-time programmable read only memory integrated circuits (PROM-ICs) includes a read data bus buffer connected between the one-time PROM-ICs and a data bus; a write data bus buffer connected between the one time PROM-ICs and the data bus; and a selection device for detecting the power supply voltage supplied to the one-time PROM-ICs and selecting one of the read data bus buffer and the write data bus buffer in response to the detected power supply voltage. The input/output control circuit improves the ability of the IC card to withstand electrostatic discharge and prevents the electrical characteristics of an IC card from changing with a change in the number of one-time PROM-ICs mounted thereon.

6 Claims, 3 Drawing Sheets



36/3,K/53 (Item 53 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011099017 **Image available**
WPI Acc No: 1997-076942/199707
XRPX Acc No: N97-063911

Circuit for detecting completed connection **of** integrated circuit card **i.e. PCMCIA type card to terminal - includes power supply** ramping **circuit which prevents voltage spikes during card insertion/extraction and supply power** detection **circuit for receiving card insertion/extraction signals**

Patent Assignee: FISET P D (FISE-I)
Inventor: FISET P D
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5589719	A	19961231	US 95401778	A	19950310	199707	B

Priority Applications (No Type Date): US 95401778 A 19950310
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5589719	A		13	H05K-001/11	

Circuit for detecting completed connection **of** integrated circuit card **i.e. PCMCIA type card to terminal...**

...**power supply ramping circuit which prevents voltage spikes during card insertion/extraction and supply power** detection **circuit for receiving card insertion/extraction signals**

...Abstract (Basic): The **IC card** circuit comprises a function generating circuit and a voltage ramping power supply (1230) for maintaining the proper sequencing of states when the **IC card** circuit is not connected to the host terminal unit. Two card **detect** sockets mate with **detect** pins of the host terminal **connector** , respectively. A card operating properly **detector** judges the ability of the **portable IC card** to function properly, responsive to the power supply and the function generating circuit...

...Two transistors receive current into their base from the **detect** pins, respectively. Two impedance devices bias the collector of the transistors to the power supply...

...terminal supplies power to the ramping power supply from the host terminal unit when the **IC card** is connected to the unit. A transistor is connected in series between the power input terminal and the internal power supply. A supply voltage **detecting** circuit receives the card insertion/extraction signal and the voltage of the ramping power supply...

...USE/ADVANTAGE - **Memory** card, SRAM, DRAM, FLASH, **EEPROM** , **EPROM** , **PROM** , hard disk drive, I/O card, communication card, video card, bus controller card, sound card, multimedia card. Provides increase in functionality and reliability by multiple uses of card **detect** signal. No voltage spikes when card is connected/ **disconnected** .

...Title Terms: **DETECT** ;

US005589719A

United States Patent [19]

Fiset

[11] **Patent Number: 5,589,719**

[45] **Date of Patent: Dec. 31, 1996**

[54] **CARD OUT OF SOCKET DETECTOR FOR IC CARDS**

[76] Inventor: **Peter D. Fiset**, 5 Upper Loudon Rd.,
Loudonville, N.Y. 12211

[21] Appl. No.: **401,778**

[22] Filed: **Mar. 10, 1995**

[51] **Int. Cl.^{6}** **H05K 1/11**

[52] **U.S. Cl.** **307/131**; 307/147; 361/737; 361/736; 439/79; 439/296

[58] **Field of Search** 307/131, 147, 307/125, 116; 361/737; 365/226; 340/825; 439/296, 79; 235/441; 361/736

[56] **References Cited**

U.S. PATENT DOCUMENTS

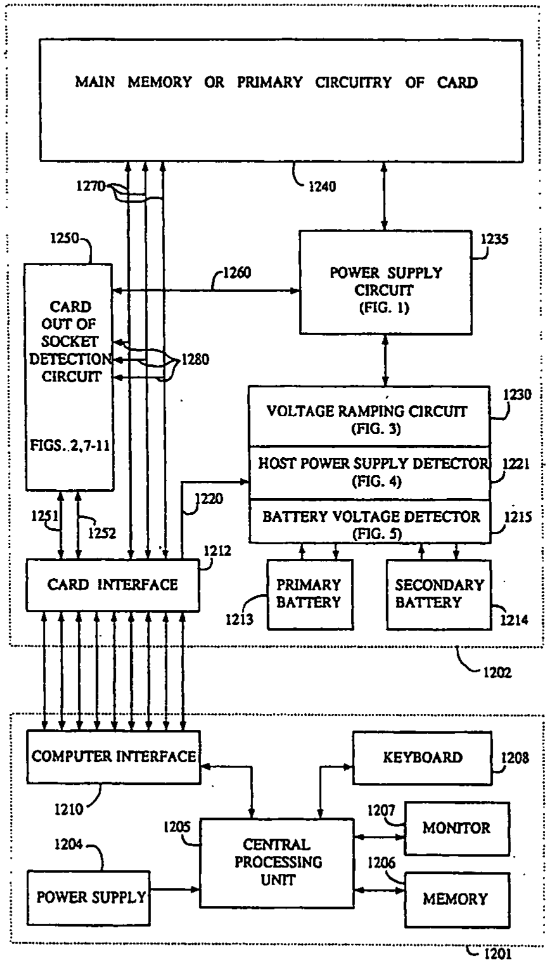
5,334,046	8/1994	Brouilette et al.	439/540
5,365,221	11/1994	Fennell et al.	340/636
5,384,492	1/1995	Carlson et al.	307/147
5,408,386	4/1995	Ringer et al.	361/785
5,451,933	9/1995	Stricklin et al.	340/825.06
5,463,261	10/1995	Skarda et al.	307/131

Primary Examiner—William M. Shoop, Jr.
Assistant Examiner—Albert W. Paladini
Attorney, Agent, or Firm—James W. Pemrick

[57] **ABSTRACT**

The present invention discloses a novel card out of socket detector circuit for IC cards, especially PCMCIA type cards. Multiple uses of the card detect signal in the IC card interface are provided. The disconnection of system pins is detected and the generation of a card out of socket response signal is created. Such as in the case of high vibration when a connection is temporarily disconnected. A power supply ramping circuit is provided so that when the IC card is connected or disconnected from the host terminal unit there are no voltage spikes within the IC card which will corrupt the operation of certain types of memory particularly in the case of voltage supply sensitive battery backed DRAM IC cards. A power supply circuit is provided which is capable of boosting a voltage from a power source. A controlled transfer from a first removable battery to a second fixed rechargeable battery is also provided that does not create excessive voltage bumps.

13 Claims, 4 Drawing Sheets



Different versions of the DRAM card can be offered. One that is to be used at room temperatures only, and another that can operate in a larger temperature range. The room temperature only card would have lower power drain because the voltage booster would be disconnected. This feature could be incorporated into a single card by throwing an external switch. The feature to power manage the voltage booster could also be incorporated into the card, with some additional power drain for the control. The voltage booster is a small drain when it is in the static state anyway, approximately 2 uA.

The comparator used in the voltage booster design could be replaced by the op-amp TLC251CD single that can go down to 1.4 volts. The TLC25L2CD dual and the TLC25L4CD quad could also be used. These parts have outputs that do not swing rail to rail and therefore would require additional active components to provide the boosted voltage.

Ultimately the easiest design would require the user to change the batteries in a powered up host. But, an equally interesting design would be to have two primary batteries. One would be used only when the replaceable was out of the circuit. This could even be a small battery that could also be replaced. In fact, replace the small one first and the large one second.

FIG. 12 shows one embodiment of the present invention illustrating the interactive operation between all the elements. The host computer **1201** is illustrated in general, showing common components typically associated with such a device. Power supply **1204** could be an external supply or a battery powered internal supply. CPU **1205** is connected to memory **1206**, display monitor **1207** and keyboard **1208**. Computer interface **1210** is a standard PCMCIA type interface having an array of pins which comply with the PCMCIA standards. Host computer **1201** is shown merely for illustration, and in no way should limit the scope of possible applications.

The IC card **1202**, which could be of the PCMCIA type, can be connected to host computer **1201** via card interface **1212**. Card interface **1212** comprises a plurality of sockets which mate with the corresponding pins of the host's computer interface **1210**. IC card **1202** includes a primary battery **1213** and a secondary battery **1214** as a power source when the IC card **1202** is not connected to host computer **1201**. Battery voltage detector **1215**, as shown in FIG. **5**, monitors the state of charge of the batteries **1213, 1214**.

Host power is supplied via signal line **1220** to the host power supply detector **1221**, as shown in FIG. **4**. This circuitry acts to recharge the primary **1213** and secondary **1214** batteries, as well as, directing power supplied from the host **1201** into the voltage ramping circuit **1230**, as shown in FIG. **3**. Voltage ramping circuit **1230** supplies power directly to the power supply circuit **1235**. This power supply circuit **1235** is illustrated by FIG. **1**. The IC card **1202** can function as a variety of devices. It could serve as a modem, external floppy drive, GPS transceiver or as an additional memory source. This memory could be volatile or non-volatile. The main functional block of the card is illustrated by numeral **1240**. The block **1240** identifies in general the specific circuitry to accomplish a given task, or a large block of memory.

The card out of socket detection circuit **1250** is connected to the card interface **1212** by signal lines **1251** and **1252**. The card out of socket detection circuit **1250** can include any one of the circuits illustrated in FIGS. **2, 7–11**. Signal line **1251** corresponds to the signal received from the CD1 pin/socket and signal line **1252** corresponds to the signal received from the CD2 pin/socket. As has been described, the card out of socket detection circuit **1250** can impress a given voltage on the CD1 and CD2 pins to simulate a specific condition. This voltage is impressed on the pins with the intent to control the IC card and the host computer. The signals received from signal lines **1251** and **1252** are also used by the card out of socket detection circuit **1250** to control the power supply circuit **1235** and the host power supply detector **1221**. When the IC card is removed, either on purpose or by accident, the signals on lines **1251** and **1252** will be the first to respond. This "early warning" is used by the card out of socket detection circuit **1250** to switch power supply from the host **1201** to the primary **1213** and/or secondary **1214** batteries. Signal line **1260** is used for data communication, control and power supply. Only one line **1260** is shown in the drawing for simplicity, but in practice there would be a plurality of connections between the power supply circuit **1235** and the card out of socket detection circuit **1250**.

Data signal lines **1270** connect the main memory/circuit **1240** of IC card **1202** to the card interface **1212**. These signal lines serve as the primary transmission path to transfer data between memory/circuit **1240** and host computer **1201**. Signal monitoring lines **1280** are connected to the data signal lines **1270**. Signal monitoring lines **1280** allow the card out of socket detection circuit to monitor the condition and state of the data signal lines **1270**. Data signals that can be monitored may include data, address, control signals and power. If one of the pins or sockets connected to the data signal lines has malfunctioned, due to vibration, dust particles, etc., the card out of socket detection circuit **1250** can identity the fault and impress a false signal on one or both of the card detect signal lines **1251, 1252** to simulate a card out of socket condition.

The present disclosure includes that contained in the appended claims, as well as that of the foregoing description. Although this invention has been described in its preferred form with a certain degree of particularity, it is understood that thc present disclosure of the preferred form has been made only by way of example and that numerous changes in the details of construction and the combination and arrangement of parts may be resorted to without departing from the spirit and scope of the invention.

What is claimed is:

1. An IC card circuit for a portable IC card selectively insertable and extractable from a host terminal unit thereby connecting and disconnecting the IC card circuit from the host terminal unit comprising,

a function generating circuit,

an internal power supply for applying a voltage to said function generating circuit to maintain the proper sequencing of states of said function generating circuit when the IC card circuit is not connected to the host terminal unit,

a first card detect socket for mating with a first card detect pin of the host terminal connector,

a second card detect socket for mating with a second card detect pin of the host terminal connector,

a card operating properly detector for detecting the ability of the portable IC card to function properly, responsive to the state of said internal power supply and responsive to the state of said function generating circuit;

a first transistor for receiving current into the base of said first transistor from the host terminal's first card detect pin,

a first impedance means for biasing the collector of said first transistor to said internal power supply, a second transistor for receiving current into the base of said second transistor from the host terminal's second card detect pin,

a second impedance means for biasing the collector of said second transistor to said internal power supply,

a logic element for outputting a card insertion and extraction signal responsive to signals from the collectors of said first transistor and said second transistor,

a power input terminal for supplying power to said internal power supply from said host terminal unit when the IC card is connected to said host terminal unit,

a power switch connected in series between said power input terminal and said internal power supply, and

a supply voltage detecting circuit for receiving said card insertion and extraction signal indicative of the connection with and disconnection from said host terminal unit and the voltage of said internal power supply for generating an output signal for the opening and closing of said power switch.

2. The IC card circuit of claim 1 wherein said power switch is a transistor.

3. The IC card circuit of claim 1 wherein said internal power supply comprises a voltage ramping power supply circuit.

4. The IC card circuit of claim 1 wherein said internal power supply comprises a voltage step up/down power supply circuit.

5. The IC card circuit of claim 1 further comprising,

a first controlled impedance means for selectively controlling current flow to the base of said first transistor, responsive to said card operating properly detector.

6. The IC card circuit of claim 5 wherein said first controlled impedance means is an analog switch.

7. The IC card circuit of claim 5 further comprising,

a second controlled impedance means for selectively controlling current flow to the base of said second transistor, responsive to said card operating properly detector.

8. The IC card circuit of claim 7 wherein said first controlled impedance means is an analog switch, and wherein said second controlled impedance means is an analog switch.

9. The IC card circuit of claim 1 further comprising,

a third controlled impedance means for selectively controlling current flow out of the emitter of said first transistor, responsive to said card operating properly detector;

a fourth controlled impedance means for selectively controlling current flow out of the emitter of said second transistor, responsive to said card operating properly detector.

10. The IC card circuit of claim 9 wherein said third controlled impedance means is an analog switch, and wherein said fourth controlled impedance means is an analog switch.

11. A portable IC card selectively insertable into and removable from a host computer interface of a host computer, thereby connecting and disconnecting the portable IC card from the host computer comprising,

a main memory or primary circuitry portion which comprises the main functional purpose of said portable IC card,

a card interface for connection to said host computer interface,

a host power supply detector circuit,

a battery voltage detector circuit,

a primary battery to supply power to said portable IC card when said portable IC card is not receiving power from said host computer,

a power supply circuit,

a plurality of data signal lines connected between said main memory or primary circuitry portion and said card interface and,

a card out of socket detection circuit connected to said data signal lines, said card interface and said power supply circuit,

said card out of socket detection circuit monitoring signals received from said card interface and said data signal lines and, selectively outputting signals to said card interface and said power supply circuit for the purpose of controlling the operation of said portable IC card.

12. The portable IC card of claim 11 where said card interface and said host computer interface are of the PCMCIA type.

13. The portable IC card of claim 11 further comprising,

a voltage ramping circuit connected between said power supply circuit and said host power supply detector.

* * * * *

```
36/3,K/38     (Item 38 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.
```

assignee

```
013494767     **Image available**
WPI Acc No: 2000-666708/200065
XRPX Acc No: N00-494147
  Security module for secure comparison of an authentication code with one
  stored in  memory  has additional auxiliary registers in which randomly
  chosen data words are placed for use in authenticating the code in the
  main registers
Patent Assignee: BULL CP8 SA (SELA  ); BULL CP8 (SELA  )
Inventor: BOLE B; SALLES J L; SALLES J
Number of Countries: 002  Number of Patents: 002
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
FR 2789774      A1  20000818  FR 991650         A   19990211  200065  B
US 6523056      B1  20030218  US 2000501999     A   20000211  200317

Priority Applications (No Type Date): FR 991650 A 19990211
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
FR 2789774    A1    19 G06F-007/06
US 6523056    B1       G06F-007/50
  Security module for secure comparison of an authentication code with one
  stored in  memory  has additional auxiliary registers in which randomly
  chosen data words are placed for use in...

Abstract (Basic):
...         is entered into some form of verifier with a code that is stored
    in secure  memory . The device includes two extra auxiliary registers
    that are used with the main registers that the security code from
    secure  memory  and the code entered to be validated in a manner to
    prevent fraudulent discovery of...
...         first sum is then calculated using these random values. The
    respective words in the main  memory  registers are compared two by two
    and then one of the words of the auxiliary...

...value equal to the first sum multiplied by the number of words in the
    main  memory  registers. When the two sums are equal the contents of
    the two main registers are...

...Means for preventing fraudulent discovery of a security code by
    monitoring  the current output from a verification device...

...Use of extra auxiliary registers and  random  code  generation  means
    that the code cannot be inferred from the current output...

...Figure shows a device for  processing   data  from a  portable  security
    device such as a  smart   card
       ...

... smart   card  (8...

... processing  verification device (1
...Title Terms:  MEMORY ;
International Patent Class (Main):  G06F-007/06 ...

... G06F-007/50
International Patent Class (Additional):  G06F-011/30 ...
```

... **G06F-012/14**
Manual Codes (EPI/S-X): **T01-E04** ...

... **T01-H01B3A** ...

... **T01-J12C**

US006523056B1

(12) United States Patent

Bole et al.

(10) Patent No.: **US 6,523,056 B1**

(45) Date of Patent: **Feb. 18, 2003**

(54) **PROCESS FOR SECURE COMPARISON OF TWO STORAGE REGISTERS, AND SECURITY MODULE IMPLEMENTING THIS PROCESS**

(75) Inventors: **Benoît Bole**, Versailles (FR); **Jean-Luc Salles**, Boulogne Billancourt (FR)

(73) Assignee: **Bull CP8**, Louveciennes (FR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/501,999**

(22) Filed: **Feb. 11, 2000**

(30) **Foreign Application Priority Data**

Feb. 11, 1999 (FR) 99 01650

(51) **Int. Cl.**[7] **G06F 7/50**; G06F 11/30

(52) **U.S. Cl.** **708/671**; 713/202

(58) **Field of Search** 708/671; 713/200, 713/210, 202

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,771,128 A		11/1973	Boardman	
5,097,260 A	*	3/1992	Ahn	340/825.56
5,226,080 A	*	7/1993	Cole et al.	235/382
5,388,212 A	*	2/1995	Grube et al.	379/118
5,416,306 A	*	5/1995	Imahata	235/380

FOREIGN PATENT DOCUMENTS

EP	0 329 966 A	8/1989
FR	2 311 365 A	12/1976
FR	2471003 A	6/1981

* cited by examiner

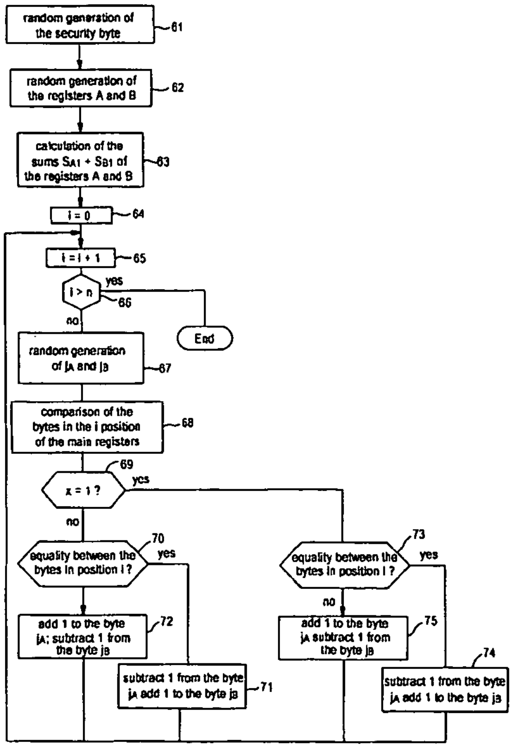
Primary Examiner—Chuong Dinh Ngo

(74) *Attorney, Agent, or Firm*—Edward J. Kondracki; Miles & Stockbridge p.c.

(57) **ABSTRACT**

The invention relates to a process for securely comparing two main storage registers, comprising defining an auxiliary storage register (A), calculating a first sum of the words composing the auxiliary storage register, comparing the words of the two main storage registers, randomly selecting one of the words of the auxiliary storage register, and modifying the value of the selected word by a first predetermined value if said words of the main storage registers are identical, and modifying the value of said selected word by a second predetermined value if said words of the main storage registers are different, calculating a second sum (S_{A2}) of the words of the auxiliary storage register, and modifying the second sum by a value equal to said first value multiplied by the number of words (n) of the main storage registers, and comparing said first and second sums (S_{A1}, S_{A2}). The invention also relates to the associated security module.

7 Claims, 4 Drawing Sheets


random generation of the security byte
61
random generation of the registers A and B
62
calculation of the sums SA1 + SB1 of the registers A and B
63
i = 0
64
i = i + 1
65
i > n
66
yes
no
End
random generation of jA and jB
67
comparison of the bytes in the i position of the main registers
68
69
x = 1 ?
yes
no
70
equality between the bytes in position i ?
yes
add 1 to the byte jA; subtract 1 from the byte jB
72
subtract 1 from the byte jA add 1 to the byte jB
71
73
equality between the bytes in position i ?
yes
no
add 1 to the byte jA subtract 1 from the byte jB
75
74
subtract 1 from the byte jA add 1 to the byte jB

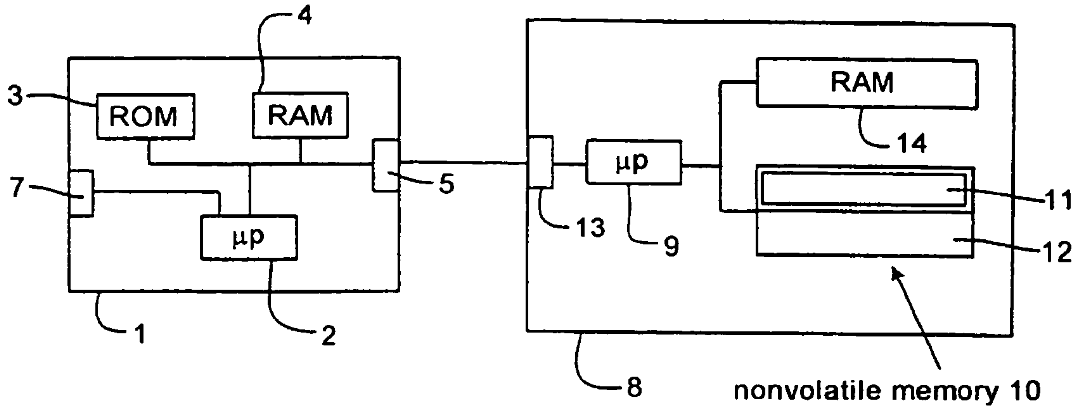

4
3
ROM
RAM
7
5
µp
1
2
RAM
14
µp
11
12
13
9
8
nonvolatile memory 10

FIG. 1

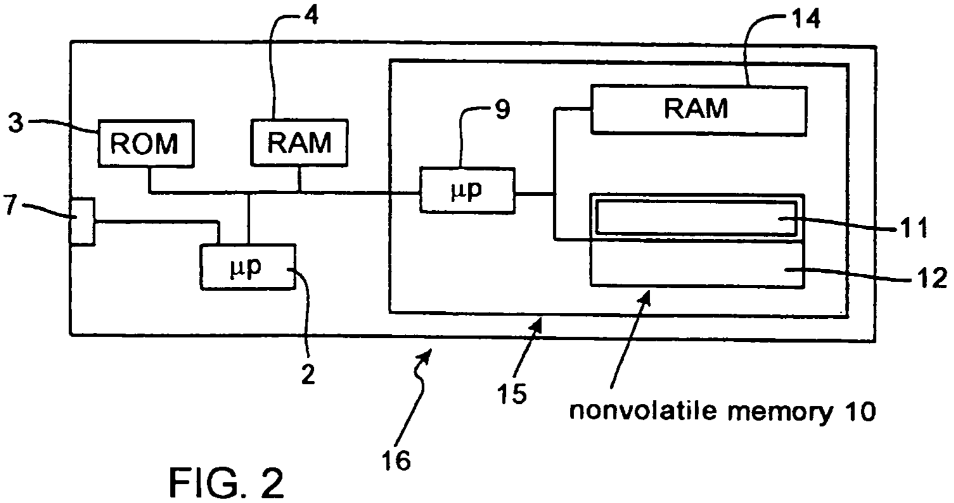

4
14
3
ROM
RAM
9
RAM
7
µp
µp
11
12
2
15
16
nonvolatile memory 10

FIG. 2

PROCESS FOR SECURE COMPARISON OF TWO STORAGE REGISTERS, AND SECURITY MODULE IMPLEMENTING THIS PROCESS

FIELD OF THE INVENTION

The invention relates to a process for the secure comparison of two storage registers, and a security module implementing this process.

DESCRIPTION OF RELATED ART

The term "security module" should be understood either in its conventional sense, in which it designates a device whose purpose in a communication or information network is to be held by an authority supervising the network and to store, in protected fashion, secret and fundamental parameters of the network such as cryptographic keys, or more simply, as designating a device allocated to various users of the network that allows each of them to have access to the latter, this latter device also being capable of holding secret parameters. The security module could take the form of a portable object of the chip card type.

It is known that a hacker is capable of deducing certain information on the operations performed in a security module by carefully studying the electric current consumption of the security module. In particular, when it comes to the operation for comparing two storage registers, the hacker can try to study the evolution of this electric current and attempt to deduce from it the positive or negative result of this comparison.

In the known art, the operation for comparing two storage registers, which is done by comparing two by two various words composing the registers, includes an operation for writing the result of each comparison performed between words: this write operation consists in a setting to 0 or to 1 of a bit in an auxiliary register, as a function of the result of the comparison. This direct translation of the result into a setting to 0 or to 1 of a bit is susceptible to being discovered by a hacker.

SUMMARY OF THE INVENTION

The object of the invention is to offer a process for comparing two storage registers that does not involve a direct writing of the result of the comparison into an auxiliary register. To this end, the invention relates to a process for comparing two main storage registers, these registers comprising the same number of words, each having a value defined by several logical elements, characterized in that it comprises the steps consisting of:

defining at least one auxiliary storage register comprising several words each having a value defined by several logical elements;

setting the logical elements of the auxiliary storage register to random values;

calculating a first sum of the values of the words of the auxiliary storage register;

comparing two by two the respective words of the main storage registers, and for each comparison of two respective words, randomly selecting one of the words of the auxiliary storage register, and modifying the value of this word by a first predetermined value if said words of the main storage registers are identical, and modifying the value of this word by a second predetermined value if said words of the main storage registers are different;

calculating a second sum of the values of the words of the auxiliary storage register, and modifying it by a value equal to said first value multiplied by the number of words of the main storage registers; and

comparing said first and second sums, and in the event of equality, declaring that said main storage registers are identical, while in the event of inequality, declaring that said main storage registers are different.

BRIEF DESCRIPTION OF THE DRAWINGS

Other details and advantages of the present invention will emerge from the following description of a preferred but non-limiting embodiment, in reference to the attached drawings in which:

FIG. 1 represents a data processing device that cooperates with a security module;

FIG. 2 represents a variant of FIG. 1;

FIG. 3 represents two main registers to be compared;

FIG. 4 represents two auxiliary registers A and B used to compare the main registers;

FIG. 5 represents a security byte used for comparing the main registers;

FIG. 6 is a flow chart of the procedure for comparing the main storage registers and accordingly writing into the auxiliary registers A and B;

FIG. 7 is a flow chart of the procedure for analyzing the result of the comparison of the main registers by means of the auxiliary registers A and B.

DESCRIPTION OF THE PREFERENCE EMBODIMENTS

FIG. 1 represents a data processing device 1 cooperating with a security module in the form of a portable object 8. The data processing device comprises, in a way that is known per se, a microprocessor 2 to which are connected a memory ROM 3 and a memory RAM 4, means 5 for cooperating, with or without physical contact, with the portable object 8, and a transmission interface 7 that allows the data processing device to communicate with a data communication network. The data processing device 1 can also be equipped with storage means such as diskettes or disks that may or may not be removable, entry means (such as a keyboard and/or a pointing device of the mouse type) and display means, these various means not being represented in FIG. 1.

The data processing device can be constituted by any computing device installed at a private or public site and capable of providing means for managing information or delivering various goods or services, this device being permanently installed or portable. It can also be a device dedicated to telecommunications.

In addition, the portable object 8 carries a chip that includes information processing means 9, a nonvolatile memory 10, a volatile working memory RAM 14, and means 13 for cooperating with the data processing device 1. This chip is laid out so as to define, in the LS memory 10, a secret area 11 in which information, once recorded, is inaccessible from outside the chip and only accessible to the processing means 9, and an accessible area 12 that is made accessible from outside the chip through the microprocessor 9 for reading and/or writing information. Each area of the nonvolatile memory 10 can comprise a part that is not modifiable ROM and a part that is modifiable EPROM, EEPROM or constituted by a RAM of the "flash" type or a

FRAM (the latter being a ferromagnetic RAM), i.e, having the characteristics of an EEPROM but with access times identical to those of a conventional RAM.

For the chip, it is possible to use a self-programmable microprocessor with a nonvolatile memory, as described in U.S. Pat. No. 4.382.279 in the name of the Applicant. As indicated in column 1, lines 13–25 of this patent, the self-programmable feature of the chip corresponds to the capability for a program fi located in a ROM to change another program fj located in a programmable memory into a program gj. In a variant, the microprocessor of the chip is replaced—or at least supplemented—by logic circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, particularly authentication and signature calculations, as a result of their hardwired, rather than microprogrammed, logic. They can particularly be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip will be designed in monolithic form.

A variant of FIG. 1 is illustrated in FIG. 2, in which the data processing device **16** comprises, in addition to the elements of the data processing device **1** of FIG. 1, those of the portable object **8** disposed in a security module **15**, the elements common to both FIGS. 1 and 2 having the same references. However, the cooperation means **5**, **13** of FIG. 1 are replaced by a permanent link between the microprocessor **2** and the microprocessor **9**.

According to a variant of FIG. 2, the data processing device is constituted by the security module **15** of FIG. 2 itself.

FIG. 3 represents two main storage registers of the volatile memory RAM **14** of the above-mentioned security module, each comprising the same number of n words constituted by (typically eight) bytes, marked (1, 2, . . . , i, . . . n). One of the two registers is a reference register that temporarily stores a reference value such as, for example, a user code or PIN (Personal Identification Number) or a signature or any other readable quantity, saved in nonvolatile memory **10** and making it possible to perform an authentication. As for the other register, it is a register to be verified by comparison with the reference register; it contains a quantity generally received from outside the security module.

The volatile memory RAM **14** also contains (FIG. 4) two auxiliary registers A, B, each comprising a certain number of bytes (typically the same number as for the main registers), marked (1, 2, . . . , j_A, . . . ,) and (1, 2, . . ., j_B . . . p). These registers will be used to record the result of the comparison between the main storage registers, as explained in reference to FIG. 6.

The volatile memory RAM **14** also contains (FIG. 5) a security byte comprising two significant bits x and y. The value of the bit x defines, as explained in reference to FIG. 6, one of two ways of translating an equality between the two main storage registers. The value of the bit y defines which of the two auxiliary registers A and B will actually be used to obtain the result of the comparison between the main storage registers.

The process for comparing the reference register and the register to be verified will now be explained in reference to FIG. 6. First of all, the security byte is generated randomly using a known random number generator provided in the hardware or software of the security module (step **61**). The two auxiliary registers A and B are also generated randomly (step **62**). Next, a first sum S_{A1} of all the bytes of the auxiliary register A and a first sum S_{B1} of all the bytes of the

auxiliary register B are calculated (step **63**). An index i defining the position of a current byte of the reference register or of the register to be verified is set to 0 (step **64**), then 1 is added to this 5 index (step **65**). i is then compared to the total number n of bytes of these registers (step **66**): if i is not greater than n, two indices j_A and j_B are generated (step **67**), j_A being between 1 and m and j_B being between 1 and p, respectively corresponding to the position of a current byte of the auxiliary register A and to the position of a current byte of the auxiliary register B.

The two bytes in the i position of the reference register and of the register to be verified are then compared (step **68**). Then, the value of the bit x of the security byte is determined (step **69**). Let us first consider the case where x is different from 1, i.e., has the value 0. In step **70**, it is first determined whether there is equality between the two bytes in position i. If not (step **72**), the byte with the index j_A of the auxiliary register A is incremented by one unit and the byte with the index j_B of the register B is decremented by one unit. If so (step **71**), the inverse operations are performed, i.e., the byte with the index j_A of the auxiliary register A is decremented by one unit and the byte with the index j_B of the auxiliary register B is incremented by one unit.

On the other hand, if in step **69**, x equals 1, the inverse operations of those performed when x equals 0 are performed. In step **73**, it is determined whether there is equality between the two bytes in position i. If not (step **75**), the byte with the index j_A of the auxiliary register A is decremented by one unit and the byte with the index j_B of the auxiliary register B is incremented by one unit. If so (step **74**), the inverse operations are performed, i.e. the byte with the index j_A of the auxiliary register A is incremented by one unit and the byte with the index j_B of the register B is decremented by one unit.

At the end of any of the four steps **71** , **72**, **74**, **75**, the process returns to step **65** to increase the index i by one unit; this is followed by a comparison of next two bytes of the reference register and of the register to be verified. Once all the bytes of these two registers have been compared, i becomes greater than n in step **66**, which ends the procedure.

The way in which the results obtained in FIG. 6 are used will be explained in reference to FIG. 7. First, the value of the bit y of the security byte is determined (step **81**). If y is different from 1, the auxiliary register A will be used to find the result of the comparison between the two main registers, and the auxiliary register B will be ignored. To do this, the sum of the bytes of the auxiliary register A is again calculated (step **82**), which gives a second sum S_{A2}. Then, the value of the bit x of the security bit is determined (step **83**). If x is different from 1, the value n is subtracted from the first sum S_{A1} of the bytes of the auxiliary register A (step **84**), i.e. this sum is modified by the value (−n). This value (−n) is obtained by multiplying by the number n of bytes of the reference register the value by which the byte j_A of the auxiliary register A was previously modified (see FIG. **6**, step **71**), or in this case (−1)x n=(−n). Lastly, in step **85**, the first and second sums S_{A1} and S_{A2} of the auxiliary register A are compared: an equality between these **10** sums indicates equality between the reference register and the register to be verified, while a difference between these two sums means that the reference register and the register to be verified are different.

If, in step **83**, x equals 1, the value n is added to the first sum S_{A1} of the bytes of the auxiliary register A (step **86**), i.e., this sum is modified by the value (+n). This value (+n) is obtained by multiplying by the number n of bytes of the